

PROSKAUER ROSE LLP

1233 Twentieth Street NW
Suite 800
Washington, DC 20036-2396
Telephone 202.416.6800
Fax 202.416.6899

NEW YORK
LOS ANGELES
BOCA RATON
NEWARK
PARIS

Jon A. Baumgarten
Member of the Firm

Direct Dial 202.416.6810
jabaumgarten@proskauer.com

October 8, 2003

Rick C. Chessen
Associate Bureau Chief
Media Bureau
Federal Communications Commission
445 Twelfth Street S.W.
Washington D.C. 20554

(Via E-Filing)

RE: MB Docket No. 02-230 (Digital Broadcast Copy Protection)

Dear Mr. Chessen

On behalf of the Motion Picture Association of America, this is in reply to your request that we provide written answers to the items indicated below.

1. **The meaning of "Downstream Product"; and the role of "Written Commitments".**

Although the terminology is understandably somewhat confusing, "Downstream Products" as defined in the proposed rules are only a subset of all products that are "downstream" from broadcast demodulators (receivers). In many cases, products that are "downstream" from the demodulators will receive digital broadcasts in digital form from a Table A output and those "downstream" devices will not be subject to FCC regulation nor to the specific "Written Commitment" requirements of the proposed rules. (They will be subject to the private license terms of the Table A technology.) In two cases, however, downstream devices may receive digital content from a demodulator via a non-Table A, self-certified "Robust Method" --- only these devices are "Downstream Products" as defined in the proposed rules; and these particular devices are subject to the proposed "Written Commitment" requirements, and to compliance with the proposed rules governing outputs and secure recording. These two cases, the applicable rules, and their evolution are described next.

Rick C. Chessen
October 8, 2003
Page 2

In the early discussions of the Broadcast Flag, the motion picture studios preferred that all digital outputs be protected by Table A technologies. The IT and CE industries, on the other hand, proposed that they be allowed to self-certify protection technologies. Self-certification, however, would create considerable uncertainty for content owners, consumers, and manufacturers alike about which products were compliant and which were not. Additionally, it inevitably risked disrupting the market, creating consumer confusion and disappointment, and frustrating content owner objectives because noncompliant products would reach the marketplace, be promoted as available, and be bought by consumers before they could be tested and, where appropriate, challenged.

As a measured compromise, the studios agreed to allow outputs from a product via a self-certified "Robust Method" in two specific situations, requested primarily by the IT industry but also of explicit interest and potential utility to CE manufacturers. The first situation involves outputs under proposed X.3 (a) (4) where the content "has not been altered following demodulation" – i.e., the content has been demodulated but has not undergone transport stream processing. (Because this content has not been processed, it could not have been examined for the Flag and will hence be "Unscreened Content", which is the subject matter of proposed section X.3.) This compromise allows IT manufacturers and others to build Demodulator Products that do not contain integrated transport stream processors. Stripping of the flag from unprocessed content is relatively difficult; and the fact that the content has not yet been processed makes it less susceptible to unauthorized interception and use than content that has been processed. The second situation is where Unscreened or processed, Marked content is passed within a computer from an add in demodulator card to an associated application under proposed section X.6(a), or over a similar add-in connection that is not an "output". Because X.6 makes clear that such content may not be passed in unencrypted, compressed form over a user accessible connection, the risks were considered acceptable to the studios. Again, the studios agreed to this limited exception to the use of Table A technologies in order to meet the expressed needs of IT and CE manufacturers for product design and configuration flexibility.

Under the proposed Compliance and Robustness Rules, devices that pass content using such a self-certified "Robust Method" in either of these two cases must do so only to products that have filed a Written Commitment with the Commission agreeing to abide

Rick C. Chessen
October 8, 2003
Page 3

by the rules, to which they then become subject.¹ This is because the rules otherwise govern only certain demodulators (and certain modulators), and the imprecise "Robust Method" formulation itself does not provide specific requirements governing output and secure recording of digital broadcast content in the Downstream Product. It is important to recognize that, at the specific design and insistence of the IT industry, this system (1) allows manufacturers to voluntarily decide whether to participate, and (2) provides significant flexibility. If manufacturers of computers or other devices "downstream" from demodulators choose not to receive demodulated digital broadcast content, they need not file Written Commitments or become subject to Commission regulation. If they do chose to participate, they may elect to either (a) receive Robust Method transfers using a self-certified technology, subject to Commission rules governing their outputs and secure recording; or (b) or use a Table A technology to obtain digital outputs of protected digital broadcast television content, subject to the terms of private licenses.

We note that in addition to the Written Commitment required for Downstream Products in the above cases, there are also Written Commitments provided for in the proposed rules in another situation. Another form of Written Commitment allows manufacturers to make non-compliant demodulation devices --- a demodulator with an unprotected digital output, for example ---and sell them to another manufacturer for incorporation into compliant products. See proposed section X.2(a)(1)(B). The sale of the non-compliant demodulator is permitted under the proposed rules because it is not made to just anyone for any purpose; instead, the buyer must be a second manufacturer that has filed a Written Commitment assuring the Commission that it is a bona fide reseller of demodulation devices and that those devices will comply with the Compliance and Robustness Requirements. This proposed rule was specifically requested by IT and CE manufacturers in order to permit flexibility in component sourcing and design---i.e. to allow the sale of noncompliant demodulation chips to other manufacturers for inclusion in a completed product that contains chips manufactured by others.²

¹ It is anticipated that an automated handshake or authentication will occur between demodulators and Downstream Products that are the subject of the Written Commitment in order to permit uninterrupted, seamless inter-operation of those devices. Thus, proposed section X.10 explicitly requires that the Robust Method be "designed to ensure that such content may be accessed in useable form by another product only if such other product is a "Downstream Product"; and the "Written Commitment" is part of the X.1 definition of "Downstream Product".

² This principle is analogous to and modeled after a common feature of other content protection systems that permit non-compliant components to be sold, but only to others who are bound by decryption licenses to incorporate them in compliant finished products. Because the Broadcast

Rick C. Chessen
October 8, 2003
Page 4

2. The cost of compliance with the Requirements.

We have been informed by manufacturers that the cost of compliance is *de minimus--- a matter of pennies---*and there is no justification for it to be otherwise. There will be a small one-time engineering charge for sketching out a compliant device, but over the entire cost of developing a new product, this is insignificant. In addition, some functionality for detecting the Flag and triggering protection will have to be added; but given the extremely simple nature of the Flag, this is hardly a significant addition to the work involved in processing the signal. Importantly, products being developed for use with secure delivery methods for pay television and other types of content will face no meaningful additional --- if any--- burden to implement compliance with the Broadcast Flag. Indeed, in the specific case of the products currently being developed for Plug & Play, no additional functionality in terms of protection technologies need be added.

3. The "DVI" exemption.

It was the studios' preference in negotiating the Broadcast Flag proposal that all digital outputs be protected. However, as already noted, in certain limited instances, balanced concessions were made at the request of some in the IT industry to accommodate specific situations. One such situation involved certain legacy computer displays manufactured with unprotected DVI 1.0 inputs. In order to permit the continued making of components that work with such products (because unprotected inputs cannot usefully process protected outputs), a narrow exemption was created in proposed sections X.3(a)(7) and X.4(a)(6) to allow limited resolution digital outputs compatible with DVI 1.0 format. This exception should not be expanded to cover other outputs, however, as it is a specific accommodation for an *already existing* and meaningful legacy. Where there is no existing, meaningful legacy, however, there is no countervailing interest to the need for protection, and thus no reason to extend the exemption.

4. Encryption at the source.

As the MPAA stated in its Reply Comments, encryption of digital broadcast content at the source is for several reasons an inferior and quite problematic solution for the problem of unauthorized redistribution. Among things, legacy DTV devices would

Flag deals with unencrypted digital broadcasts, in this case the Written Commitment plays the role of the decryption license.

Rick C. Chessen
October 8, 2003
Page 5

be rendered useless, it would be necessary to deal with thorny intellectual property issues associated with proprietary encryption and authentication schemes, and inevitable protracted delay would accompany designing and selecting an encryption scheme and then implementing it via a Commission rulemaking. We estimate that this process could take 5 years or more, in the interim subjecting broadcast content to ever increasing amount of unauthorized redistribution, stopping the DTV transition in its tracks, and chilling new development as companies wait to see what the ultimate rules are. Additionally, because this approach would require licensed decryption technologies in every product receiving over-the-air broadcasts, it would likely be far more expensive than the Broadcast Flag system.

5. Section 1201(c)(3) of the Digital Millennium Copyright Act.

The assertion by some that Section 1201(c)(3) of the Copyright Act has a negative bearing on the Commission's actions here is ludicrous. Section 1201(c)(3) by its own terms applies only to "this section" – that is, Section 1201 of Title 17. It does not have any application outside of Section 1201, and particularly not to the Commission's authority under Title 47. Additionally, the purpose of this provision was to avoid the possibility that to defeat claims of circumvention, manufacturers might have to build responses into their products to every possible undefined, non-specific technological protection measure that might ever be adopted at the unilateral whim or dictate of any content owner. It certainly did not state or reflect a Congressional policy against specific, defined technological mandates under government authority; to the contrary, section 1201(k) of the very same DMCA requires compliance with just such a specific mandate and if anything, establishes the existence of Congressional policy in favor of such specific and carefully tailored mandate.

6. Effective date in relation to Plug and Play.

Because no *additional* protection will be required under the Broadcast Flag than is required for subscription content under the Commission's forthcoming Plug & Play order, there should be absolutely no difference between the effective dates for Plug & Play products generally and for Broadcast Flag-complaint Plug & Play devices. To conclude otherwise will foster an instant, expanding and enduring legacy of Plug & Play devices that are encouraged to enter the market by the Commission's activities in that proceeding, yet inexplicably treat digital broadcast content in unprincipled fashion as somehow unworthy of protection against the severe problems of unauthorized redistribution.

Rick C. Chessen
October 8, 2003
Page 6

In the case of non-Plug & Play devices of the same type sold today, an effective date for Broadcast Flag compliance of July, 2005 would be appropriate; however it must be clear that manufacturers cannot flood the market with non-compliant devices to take advantage of this transition.

The pertinence of the Plug & Play proceeding to the Broadcast Flag issue is apparent in other respects as well. As noted in item 2 above, the Flag implementation costs in Plug & Play devices that will already have Table A protected outputs are immaterial. More fundamentally, in its Plug & Play proceeding the Commission will review, approve, enact and oversee compliance, robustness, and copy protection rules for subscription television that are substantially indistinguishable ---except to the extent they are more restrictive, for example, with respect to recording---from the proposed Broadcast Flag rules. Surely, given its commitment to the DTV transition, the FCC will not subscribe to the indefensible second class treatment of broadcast content that is instrumental to that very transition.

7. Cable and satellite compatibility.

Every effort was made in the proposed Broadcast Flag regulations to accommodate the flexibility of cable and satellite systems to implement the Flag in the way that worked best for them in any particular case, system or structure. Under section X.2 (d) & (e) of the proposed rules, cable and satellite providers that intercept and retransmit digital broadcast signals from over-the-air broadcasts must (1) if they encrypt the content after demodulation, check for the Flag before encryption, convey the Flag's information to the consumer's set-top box, and require that the consumer product, upon decryption, protect the content in accordance with the proposed demodulator rules; or (2) if they do not encrypt the content, preserve the Flag if present, and retransmit the flagged content in n-VSB or m-QAM modulated form, in which case the consumer's receiving apparatus will comply with the rules pertaining to demodulators.

8. News and public affairs.

Some commentators have called for a bar to news and public affairs programming being marked with the Flag. There are several problems with this proposal. First, news and public affairs programs are not necessarily any less expensive or creative to produce, nor subject of less fruitful secondary markets, territorial commercial support, or migration to more secure channels than other programming, and thus may be subject to the same business and public concerns over unauthorized redistribution that create the

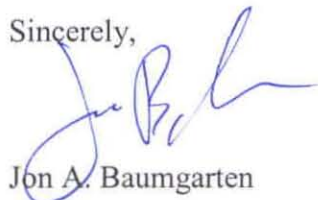
PROSKAUER ROSE LLP

Rick C. Chessen
October 8, 2003
Page 7

need for the Broadcast Flag.³ Second, news and public affairs programming in particular may be the primary original content created by many local broadcasters, meaning that an exemption would fall disproportionately hard on that segment of content owners, and that this programming may be particularly impaired by unauthorized wide redistribution. Third, there are insuperable definitional problems with such an exemption. Who will decide what is a news or public affairs program? Will it have to be done on a case-by-case basis? Is Howard Stern's show a news program? What about "Entertainment Tonight," or "Access Hollywood"? Such an exemption would require the FCC to make continual content-based distinctions. Finally, any notion that video clipping services would benefit from such an exemption is belied by the fact that such services even now, under established case law and industry practice need broadcasters' permission to reproduce and market their excerpts; the Flag would not alter this requirement.

Please let us know if you have additional questions concerning the above.

Sincerely,



Jon A. Baumgarten

JAB/clt

CC: Secretary Marlene H. Dortch

³ See the discussion of this need in the Joint Initial Comments of the MPAA *et al* in MB Docket 02-230 at Part I (Dec. 6, 2002) and the Joint Reply Comments of the MPAA *et al* in that Docket at Part I A (Feb. 20, 2003).